Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89
	)	
	)	

REPLY COMMENTS OF
MOTOROLA SOLUTIONS, INC.

Motorola Solutions, Inc. ("MSI") respectfully submits these reply comments in the above-captioned proceeding.[1] MSI reiterates its support for the efforts of the Federal Communications Commission ("FCC" or "Commission") to promote the security and integrity of the nation's communications networks. More than 20 parties filed comments in this proceeding, expressing concern over a wide range of issues implicated by the Commission's Notice of Proposed Rulemaking.

In its comments, MSI supported the Commission's efforts to respond to critical supply chain vulnerabilities by adopting the necessary rules and policies to prevent USF funds from being used to purchase or obtain equipment or services produced or provided by companies that pose a risk to national security and the integrity of communications networks or the communications equipment supply chain.[2] MSI also noted that the Commission should publish a list of prohibited suppliers to inform the communications industry and other stakeholders, developed by Congress as well as executive branch agencies with the appropriate security-based

---

1 Notice of Proposed Rulemaking, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, FCC 18-42 (April 18, 2018) ("Notice").

2 Comments of Motorola Solutions, Inc., WC Docket No. 18-89 (filed Jun. 1, 2018), at 2.

expertise in a whole-of-government approach.[3] Congress is already taking action in furtherance of this approach; the House of Representatives recently passed H.R. 5515, the National Defense Authorization Act for Fiscal Year 2019, which includes a provision that would require the Director of National Intelligence to develop a report in coordination with the Director of the FBI, and the Secretaries of State, Homeland Security, and Defense, detailing the threats to national security posed by Huawei Technologies Company, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, or ZTE Corporation, with particular emphasis on any evidence of malicious software or hardware that would enable unauthorized network access or control.[4] Additionally, H.R. 5515 will take the important step of making an unclassified version of the Director of National Intelligence's report available to state and local governments with impacted telecommunications companies.[5]

Other comments filed in this proceeding echo MSI's in support of a whole-of-government approach. The Telecommunications Industry Association ("TIA") recommended the Commission publish a list of prohibited suppliers "derive[d] from determinations made by agencies with appropriate national security expertise, or by Congress…recogniz[ing] that the Commission does not have appropriate expertise to make supplier-specific national security determinations on its own, and that such independent determinations could result in an inconsistent patchwork of restrictions by different agencies across the government."[6] USTelecom agreed that the Commission would be better served consulting other agencies and

---

3 *Id*. at 3-4.

4 National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong. (2018), at §880(c)(1). H.R. 5515 was passed by the House of Representatives on May 24, 2018, and is currently being considered in the Senate.

5 *Id*. at § 880(c)(2).

6 Comments of TIA, WC Docket No. 18-89 (filed Jun. 1, 2018), at 54.

leveraging their expertise to inform the Commission's list: "Supply chain risk lives at the intersection of vulnerabilities and threats; the FCC is not in a position to actively determine either on its own. The Commission has not previously demonstrated an independent capability to examine and evaluate technical vulnerabilities in the communications supply chain."[7] Likewise CTIA's comments recommended the Commission take advantage of ongoing efforts by other agencies, particularly DHS, which recently announced initiatives to conduct supply chain security risk assessments in the communications sector, and which could serve as a launching point for broader interagency coordination in protecting supply chains across a range of sectors.[8]

MSI also recommended that the Commission formulate definite criteria illustrating why a company would be included on the list, in order to ensure a measure of consistency and transparency to the process as well as protect against concerns that the criteria for inclusion are unnecessarily overbroad.[9] TIA also advocated for well-defined criteria to anchor the policy discussion and shed light on what factors the Commission wanted to emphasize. In particular, TIA proposed three categories of criteria to assist identifying suppliers of concern: nation-specific criteria, highlighting risks associated with countries with a demonstrated history of state-sponsored cyberespionage; company-specific criteria, where individual companies have a record of illegal activity or receive support from states of concern; and product-specific criteria, in order to differentiate the different levels of scrutiny inherent in particular products, the customers who use them, and the use cases specific to those products.[10] Similarly, CTIA argued that the Commission should "provide clear guidance to the Universal Service Administrative Company

---

7 Comments of USTelecom, WC Docket No. 18-89 (filed Jun. 1, 2018), at 9.

8 Comments of CTIA, WC Docket No. 18-89 (filed Jun. 1, 2018), at 8.

9 Comments of Motorola Solutions, Inc., at 4.

10 Comments of TIA, at 82-84.

(USAC) regarding its role in implementing, overseeing, and enforcing any restrictions or prohibitions that arise from this proceeding."[11] MSI agrees that the Commission must ensure that any terms it creates to define what vendors should or should not be placed on a list of prohibited suppliers are clear and consistent in order to adequately encompass those companies that pose a threat to U.S. communications supply chains now as well as ensure new threats are quickly identified and included.

Significantly, MSI also explained the necessity of the Commission expanding the scope of its inquiry to encompass public safety communications such as land mobile radio, Next Generation 9-1-1, and FirstNet, given their unique and critical importance, and the fact that under the Commission's current framework, these communications remain vulnerable to such threats.[12] MSI strongly recommends the Commission pursue further rulemaking proceedings to address the importation as well as marketing of any technology intended for public safety use that is designed, supplied, or manufactured by companies that present a threat to our national security and the integrity of U.S. communications networks. In their comments, AT&T argued that applying restrictions to all telecom and information network operators was necessary to effectively protect communications supply chains.[13]

With this rulemaking, the Commission is taking action to protect our nation's communications networks and its communications supply chain. There is strong consensus that the proposal to prohibit the use of USF funds to purchase equipment or services from any providers that pose a national security risk is a meaningful and worthwhile step toward

---

11 Comments of CTIA, at 19.

12 Comments of Motorola Solutions, Inc., at 5.

13 Comments of AT&T Services, Inc., WC Docket No. 18-89 (filed Jun. 1, 2018), at 3.

protecting the integrity of our networks. However while the Commission's proposal can potentially benefit some aspects of public safety communications, the Commission should take the opportunity to more directly target supply chain vulnerabilities affecting public safety communications that would not be necessarily covered by a rule that only encompasses the USF.

Respectfully Submitted,

/S/ Frank Korinek
Frank Korinek
Director of Government Affairs
Spectrum and Regulatory Policy
Motorola Solutions, Inc.
1455 Pennsylvania Avenue NW
Suite 900
Washington, DC 20004
(202) 371-6900

July 2, 2018